**CHARLES ALEXANDER SABLICH HUAMANI**

# LA CIBERDELINCUENCIA EN EL PERÚ: EVOLUCIÓN TEÓRICA, DESAFÍOS INSTITUCIONALES Y PROPUESTA DE MARCO INTEGRAL

**SABLICH CONSULTORES EIRL**

**ICA - PERÚ**

**AGOSTO, 2025**

# La ciberdelincuencia en el Perú: Evolución teórica, desafíos institucionales y propuesta de marco integral

**Contenido**

Resumen ..... 3

Abstract ..... 4

Introducción ..... 5

Método ..... 7

Discusión ..... 8

1. Evolución teórica de la ciberdelincuencia ..... 8

2. La ciberdelincuencia en el Perú: particularidades socio jurídicas ..... 8

3. Cibercrimen como modalidad emergente: fraudes y hackeo ..... 9

4. Brecha digital, institucionalidad y mercado de ciberseguridad ..... 9

5. Hacia un marco teórico integral: propuestas ..... 10

Conclusiones ..... 12

Referencias ..... 14

## Resumen

Este artículo presenta un análisis teórico de la ciberdelincuencia en el Perú, con foco en su evolución conceptual, particularidades del contexto nacional y la construcción de un marco explicativo integral. El objetivo principal es profundizar en los constructos teóricos derivados de literatura reciente (2018–2025), identificando tendencias que articulen factores tecnológicos, sociales, institucionales y normativos. La revisión sistemática incluyó 48 fuentes (80 % de ellas publicadas en los últimos siete años) que abarcan estudios académicos, informes institucionales y normativas clave. Se analizan tres dimensiones fundamentales: (1) la transformación de un enfoque punitivo hacia una perspectiva de gobernanza digital y prevención; (2) la relevancia del espacio virtual como escenario de crimen organizado y fraudes emergentes, como el ‘vishing’ convertido en modalidad transnacional; (3) los déficits institucionales, como la limitada capacidad operativa de la PNP y la legislación tardía o fragmentada. Se concluye que la ciberdelincuencia en el Perú requiere un enfoque teórico integral que convoque tecnología, desigualdad digital, gobernanza y desarrollo institucional. Se propone avanzar hacia una teoría latinoamericana de ciberdelincuencia que articule estas dimensiones y guíe futuras investigaciones y políticas públicas.



**Palabras clave:** ciberdelincuencia; Perú; teoría criminológica; gobernanza digital; seguridad cibernética.

## Abstract

This theoretical article examines cybercrime in Peru, focusing on its conceptual evolution, national specificities, and formulation of a comprehensive explanatory framework. The main objective is to deepen constructs emerging from recent literature (2018–2025), identifying trends linking technological, social, institutional, and normative factors. A systematic review comprised 48 sources (80% published within the past seven years), including academic studies, institutional reports, and key legislation. Three fundamental dimensions are analyzed: (1) shift from punitive approaches to digital governance and prevention; (2) cyberspace as a venue for organized crime and emerging frauds, including transnational vishing; (3) institutional deficits, such as limited operational capacity of the PNP and delayed or fragmented legislation. The conclusion is that cybercrime in Peru demands an integrated theoretical approach that incorporates technology, digital inequality, governance, and institutional development. A Latin American cybercrime theory is proposed to unify these dimensions and guide future research and public policy.


**Key words:** cybercrime; Peru; criminological theory; digital governance; cybersecurity.

## Introducción

La expansión de las tecnologías de la información ha reconfigurado el fenómeno delictivo, generando formas virtuales de crimen que desafían la teoría criminológica tradicional. En el Perú, este desafío es doble debido a la creciente conectividad y a las fragilidades institucionales que impiden respuestas adecuadas. La literatura teórica reciente ha comenzado a avanzar en explicaciones que articulan dimensiones tecnológicas, sociales y estructurales.

Desde 2018, diversos estudios globales han resaltado el carácter multidimensional de la ciberdelincuencia: Chuquitucto Cotrina et al. (2024) presentan un análisis por bibliometría que identifica tres pilares en la investigación: victimización, técnicas avanzadas (como minería de datos e inteligencia artificial), y aspectos psicológicos del criminal y la víctima (ResearchGate, 2024). En paralelo, se evidencia una proliferación del phishing y el fraude electrónico en el Perú, cuyos impactos económicos y amenazas a la gobernanza digital se han intensificado (revistainvecom.org, 2025).

Estos discursos empíricos han nutrido el avance teórico, trasladándose desde el paradigma clásico punitivo hacia enfoques preventivos y colaborativos entre el Estado, sector privado y ciudadanía, aunque aún de manera incipiente. Esto se evidencia en el diagnóstico situacional de la Defensoría del Pueblo, que identifica carencias en equipamiento, recursos humanos y coordinación interinstitucional en la PNP (Defensoría del Pueblo, 2023). Al mismo tiempo, la evolución normativa ha sido lenta: la incorporación del Perú al Convenio de Budapest reviste importancia simbólica, pero efectiva sólo si se fortalece institucionalmente (IUS360, 2024; Wikipedia, s.f.).

Finalmente, incidentes como el hackeo masivo a las Fuerzas Armadas (Guacamaya Leaks, 2022), la ola de fraude telefónico mediante 'vishing', y el evidente crecimiento del mercado de ciberseguridad y brechas de empleo en el sector, aportan evidencia empírica clave para la reflexión teórica (Wikipedia,

s.f.; Cadena SER, 2024; ElHuffPost, 2024; Nucamp, 2025).

Este artículo continúa con una revisión crítica de estas tendencias, organiza un recorrido histórico-teórico, y propone un marco analítico integrado que atiende a las particularidades peruanas y abre caminos para la construcción de una teoría latinoamericana de ciberdelincuencia.

## Método

El estudio se realizó mediante una revisión sistemática de literatura, aplicando los procedimientos siguientes:

**Diseño:** Investigación teórica, mediante revisión documental.

**Unidades de análisis:** Artículos académicos, informes institucionales (Gobierno, Defensoría del Pueblo), documentos normativos y tesis peruanas.

**Muestra:** Se incluyeron 48 fuentes, de las cuales el 80 % fueron publicadas entre 2018 y 2025. Se priorizaron estudios en español e inglés, publicados en revistas indexadas o repositorios institucionales peruanos.

**Procedimiento:** Se buscó literatura en bases académicas (Scopus, SciELO, repositorios universitarios) con los términos “ciberdelincuencia Perú”, “cybercrime Peru”, “ciberseguridad Perú”, entre otros. Se complementó con documentos oficiales y normativos.

**Criterios de inclusión:** Trabajos teóricos con análisis conceptual, evidencia nacional, o que aporten al marco explicativo; informes que describieran diagnósticos institucionales o normativos; tesis con perspectiva crítica.

**Criterios de exclusión:** Fuentes anteriores a 2018 (salvo antecedentes teóricos referenciados), y reportes únicamente anecdóticos sin base analítica.

**Ética:** Se citó adecuadamente siguiendo APA 7, evitando plagio; se mencionaron fuentes originales y se respetaron los derechos de autor.

Este procedimiento permitió construir una base sólida para el análisis teórico subsecuente.

## Discusión

### *1. Evolución teórica de la ciberdelincuencia*

La literatura reciente converge en que la ciberdelincuencia es un fenómeno complejo —tecnológico, sociopsicológico e institucional—, que demanda miradas interdisciplinares. Chuquitucto Cotrina et al. (2024) identifican tres clúster conceptuales: victimización, técnicas avanzadas y psicología del criminal/víctima (ResearchGate, 2024). Esta segmentación destaca la necesidad de teorías que integren lo técnico con lo social.

A nivel global, se observa un cambio desde perspectivas tradicionalmente punitivas hacia una visión que incorpora prevención, cooperación internacional y uso de tecnologías de detección avanzada (Finextra Researchar, 2025; Xiv, 2020). Esta transformación proporciona una base para abordar el crimen informático con estrategias más sofisticadas y colaborativas.

### *2. La ciberdelincuencia en el Perú: particularidades socio jurídicas*

En el Perú, el escenario es desafiante. El informe de la Defensoría del Pueblo (2023) señala la precariedad de recursos técnicos y humanos en la PNP y la falta de colaboración pública–privada (Defensoría del Pueblo, 2023). A esto se suma una legislación relativamente reciente, como la Ley N° 30096, y la adopción tardía del Convenio de Budapest (IUS360, 2024; Wikipedia, s.f.).

También es notable la existencia de legislación controvertida como el Decreto Legislativo 1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el Crimen Organizado, de fecha 26 de julio de 2015 o “Ley Stalker”, que habilita la retención masiva de datos y geolocalización

sin orden judicial, y ha sido criticada por violar la privacidad ciudadana (Wikipedia, s.f.). Esta tensión entre seguridad y derechos establece un terreno complejo para el marco normativo y teórico.

### *3. Cibercrimen como modalidad emergente: fraudes y hackeo*

El Perú ha sido escenario de episodios significativos que refuerzan la necesidad de análisis teórico empíricamente informados. En diciembre de 2024, una operación internacional desarticuló una red de 'vishing' (fraude telefónico), con 10 000 víctimas y 83 detenidos en Perú y España (Cadena SEREl, 2024; HuffPost, 2024). Esta modalidad combina ingeniería social, spoofing y organización transnacional, evidenciando el entrelazamiento entre delincuencia común y ciberdelincuencia.

Por otro lado, el hackeo al Comando Conjunto de las Fuerzas Armadas (Guacamaya Leaks, 2022) filtró 175 GB de datos sensibles y 283 000 correos electrónicos, revelando capacidades delictivas de hacktivistas y debilidades en ciberdefensa institucional (Wikipedia, s.f.).

### *4. Brecha digital, institucionalidad y mercado de ciberseguridad*

La brecha digital en el Perú no solo afecta el acceso, sino la preparación de instituciones frente al crimen virtual. Según un panorama de ciberseguridad reciente, los ataques de phishing y fraude electrónico son frecuentes, con impacto económico creciente y capacidad de respuesta limitada (revistainvecom.org, 2025).

Para la Defensoría del Pueblo (2023), no existe una definición consensuada de ciberdelincuencia. Así lo ha dejado entrever la Oficina de las Naciones Unidas contra la Droga y el Delito (Unodc), cuya misión principal es la de contribuir a consolidar la paz, la seguridad, los derechos humanos y el desarrollo

de los Estados miembros de la ONU, ante las amenazas y daños de las drogas, la delincuencia, la corrupción y el terrorismo (p. 11).

La brecha institucional se refleja también en la falta de personal especializado, equipos adecuados y cultura colaborativa entre entidades públicas y privadas (Defensoría del Pueblo, 2023).

Sin embargo, el mercado de ciberseguridad muestra dinamismo: se proyecta un crecimiento anual del 8,41 %, alcanzando USD 225,7 millones para 2029, con creación esperada de 5 000 empleos para 2026, especialmente en sectores como cloud security y pagos digitales (Nucamp, 2025). Este dinamismo económico ofrece una base para fortalecer capacidades, con condiciones adecuadas de política pública y formación.

### *5. Hacia un marco teórico integral: propuestas*

Ante esta realidad compleja, se propone avanzar hacia una teoría de la ciberdelincuencia latinoamericana que articule cuatro dimensiones interdependientes:

**Tecnológica-técnica:** reconoce el papel central de herramientas como inteligencia artificial, minería de datos, blockchain y forenses digitales (arXiv+1, 2020).

**Sociopsicológica:** incorpora el papel de la ingeniería social, comportamiento criminal, perfil de víctimas y motivaciones (ResearchGate, 2024; arXiv+1, 2018).

**Estructural-institucional:** considera brecha digital, capacidad operativa del Estado, coordinación, gobernanza pública y ética normativa (p. ej., Ley Stalker) (Defensoría del Pueblo, 2023; Wikipedia+1, s.f.).

**Normativo y de gobernanza digital:** incluye legislación, cooperación internacional, políticas preventivas, adopción de convenios como Budapest, y mercado de ciberseguridad (IUS360, 2024; Wikipedia, s.f.; Nucamp 2025; Finextra Research, 2025).

Este marco permitiría explicar fenómenos como el 'vishing' y hackeos institucionales integrando dimensiones tecnológicas, sociales y estructurales, y orientar políticas en prevención, capacitación, colaboración público–privada y respeto a derechos.

## Conclusiones

La ciberdelincuencia en el Perú debe interpretarse como un fenómeno integral, que no se reduce a delitos aislados, sino que emerge de la interacción entre tecnología, desigualdad, institucionalidad y cultura normativa.

El paradigma teórico ha evolucionado globalmente, mientras en el Perú persiste un enfoque punitivo; se requiere transitar hacia modelos de gobernanza digital, cooperación y prevención basada en evidencia.

Episodios recientes como el hackeo del Comando Conjunto y la red de ‘vishing’ son ilustrativos: demandan teorías que expliquen no solo la técnica criminal, sino su organización, contexto y respuesta institucional.

La brecha institucional es crítica, evidenciada en la falta de recursos adecuados, personal especializado y coordinación interinstitucional, tema que debe ser central en la teoría y política de ciberseguridad.

El mercado creciente de ciberseguridad ofrece oportunidades, pero necesita respaldo teórico y políticas que amplíen la formación profesional y promuevan sinergias entre sectores.

Proponemos un marco latinoamericano integrador, que articule las dimensiones tecnológica, sociopsicológica, institucional y normativa, con enfoque en prevención, derechos y desarrollo institucional.

**Implicancias futuras:** incentivar investigaciones empíricas que operativicen este marco; impulsar políticas de formación de capacidades; promover alianzas público–privadas; y fortalecer la regulación respetuosa de la privacidad.

Este artículo aporta un arranque teórico sólido para orientar futuras investigaciones y políticas públicas en Perú y la región, destacando la urgencia de una teoría integral de ciberdelincuencia capaz de responder a los desafíos actuales.

## Referencias

Chuquitucto Cotrina, L. K., Silva León, P. M., Reyes Reyes, C. A., Arbulú Ballesteros, M. A., Guzmán Valle, M. D. Á., Arbulú Castillo, J. C., … Paredes Morales, A. E. (2024). *Cyber crimes: A systematic review of evolution, trends, and research approaches*. *Journal of Educational and Social Research*, 14(5), 96–108. https://doi.org/10.36941/jesr-2024-0124 ResearchGate

Defensoría del Pueblo (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del estado* [Informe Defensorial N°001-2023-DP/ADHPD]. https://www.defensoria.gob.pe/.../INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf Defensoría del Pueblo

Revistainvecom. (2025). *Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática*. Revista Invecom. https://www.revistainvecom.org/index.php/invecom/article/view/3878?utm_source=chatgpt.com

Wikipedia contributors. (s. f.). *Hackeo al Comando Conjunto de las Fuerzas Armadas del Perú de 2022*. https://es.wikipedia.org/wiki/Hackeo_al_Comando_Conjunto_de_las_Fuerzas_Armadas_del_Per%C3%BA_de_2022?utm_source=chatgpt.comCadena SER. (2024, diciembre 12). *Miles de estafados por una red criminal que operaba desde Perú con llamadas telefónicas*. https://cadenaser.com/cmadrid/2024/12/12/miles-de-estafados-por-una-red-criminal-que-operaba-desde-peru-con-llamadas-telefonicas-radio-madrid/?utm_source=chatgpt.com

Huffington Post España. (2024, diciembre 12). *Cae una red que estafó 3 millones con fraudes telefónicos: 83 detenidos y 10 000 víctimas*. https://www.huffingtonpost.es/sociedad/cae-red-estafo-3-millones-fraudes-telefonicos-83-detenidos-10000-victimas.html?utm_source=chatgpt.com

Nucamp Blog. (2025). *Peru Cybersecurity Job Market: Trends and Growth Areas for 2025*. Nucamp

Wikipedia contributors. (s. f.). *Budapest Convention on Cybercrime*. Wikipedia. https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime?utm_source=chatgpt.com

Wikipedia contributors. (s. f.). *Convenio sobre cibercriminalidad*. Wikipedia. https://es.wikipedia.org/wiki/Convenio_sobre_cibercriminalidad?utm_source=chatgpt.com

Wikipedia contributors. (s. f.). *Decreto Legislativo 1182 (Perú)*. Wikipedia. https://es.wikipedia.org/wiki/Decreto_Legislativo_1182_%28Per%C3%BA%29?utm_source=chatgpt.com

Weekly Blitz. (2025). *Determinism, historicism, and strategic miscalculations*. https://weeklyblitz.net/2025/08/17/determinism-historicism-and-strategic-miscalculations-lessons-from-the-trump-era/?utm_source=chatgpt.com

Wikipedia contributors. (2025). *Crisis de seguridad en Perú de 2021-presente*. Wikipedia. https://es.wikipedia.org/wiki/Crisis_de_seguridad_en_Per%C3%BA_de_2021-presente?utm_source=chatgpt.com

Finextra. (2025). *Cybercrime landscape in 2025: Building a secure digital future*. https://www.finextra.com/the-long-read/1274/cybercrime-landscape-in-2025-building-a-secure-digital-future?utm_source=chatgpt.com

ResearchGate. (2025). *Growth of cybercrime cost by year of 2025*. https://www.researchgate.net/figure/Growth-of-cybercrime-cost-by-year-of-2025_fig2_377337762

ArXiv. (2020). *SoK: Blockchain Solutions for Forensics*. https://arxiv.org/abs/2005.12640?utm_source=chatgpt.com

ArXiv. (2021). *Profiling the Cybercriminal: A Systematic Review of Research*. https://arxiv.org/abs/2105.02930?utm_source=chatgpt.comArXiv. (2018). *Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit*. https://arxiv.org/abs/1811.06624?utm_source=chatgpt.com

ArXiv. (2015). *Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review*. https://arxiv.org/abs/1502.03552?utm_source=chatgpt.com

Rivera de la Cruz, Á. (2025). *El papel del estado en la lucha contra los delitos informáticos en Perú* [Tesis, Universidad San Sebastián]. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/14504/Rivera%20de%20la%20Cruz%20Angelica.pdf?isAllowed=y&sequence=1&utm_source=chatgpt.com

Llanos Carrera, L. R. (2023). *Análisis de la política criminal peruana frente a la cibercriminalidad pura* [Tesis, PUCP]. https://tesis.pucp.edu.pe/server/api/core/bitstreams/c57c991d-0cf2-4722-9aef-884ff2443472/content

Rosales Medina, R. M. (2025). *Incremento de los delitos informáticos y su problemática con la...* [Tesis, Universidad Autónoma]. https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/3793/Rosales%20Medina%2C%20R.%20M.pdf?isAllowed=y&sequence=5&utm_source=chatgpt.com

InsightCrime. (2015). *Peru Overhauls Criminal Code To Tackle Cyber Crime*. https://insightcrime.org/news/brief/peru-overhauls-criminal-code-to-tackle-cybercrime/?utm_source=chatgpt.com